L1: Entry 24 of 45 File: USPT Jan 20, 2004

DOCUMENT-IDENTIFIER: US 6680922 B1
TITLE: Method for the recognition and operation of virtual private networks (VPNs) over a wireless point to multi-point (PtMP) transmission system

Abstract Text (1):
A packet-centric wireless point to multi-point telecommunications system includes a wireless base station coupled to a first data network; one or more host workstations coupled to the first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with the wireless base station over a shared wireless bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of the subscriber CPE stations over a second network; resource allocator optimizing end-user quality of service (QoS) and allocating shared bandwidth among the subscriber CPE stations; a scheduler to schedule an internet protocol (IP) flow over the shared wireless bandwidth. The scheduler includes a prioritizer for prioritizing the IP flow based on priorities of a virtual private network (VPN). The system can include an analyzer for analyzing the virtual private network (VPN) priorities for the IP flow, or for prioritizing all VPN IP flows. The system can include a prioritizer to prioritize the IP flow based on one or more subscriber-defined parameters. In the system, the VPN can include a directory enabled networking (DEN) table management scheme. The VPN can be implemented using a point-to-point tunneling protocol (PPTP). Also included is a method for accomplishing the above.

Brief Summary Text (6):
Wireless networks present particular challenges over their wireline counterparts in delivering QoS. For example, wireless networks traditionally exhibit high bit error rates (BER) due to a number of reasons. Conventional wireless networks also implement circuit switched connections to provide reliable communications channels. However the use of circuit switched connections allocates bandwidth between communicating nodes whether or not traffic is constantly being transferred between the nodes. Therefore, circuit switched connections use communications bandwidth rather inefficiently.

Brief Summary Text (12):
The present invention is directed to a packet-centric wireless point to multi-point telecommunications system, including: a wireless base station coupled to a first data network; one or more host workstations coupled to the first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with the wireless base station over a shared bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of the subscriber CPE stations over a second network; resource allocation means optimizing end-user quality of service (QoS) and allocating shared bandwidth among the subscriber CPE stations; a means for analyzing and scheduling an internet protocol (IP) flow over the shared wireless bandwidth.

Detailed Description Text (15):
To provide a non-ambiguous definition of QoS that applies to wireless data communications, the nature of the problem that QoS is meant to solve is helpful. Many of the problems of data communications over wireless are unique and distinct from those of wireline data communications, while some are in fact shared. For

wireless broadband access systems, the problems of quality delivery are somewhat more complex than for the wireline analog. Like its wireline counterpart, the problems encountered in wireless delivery of data include, e.g., slow peripheral access, data errors, "drop-outs," unnecessary retransmissions, traffic congestion, out-of-sequence data packets, latency, and jitter. In addition to these problems, wireless delivery adds problems including, e.g., high inherent bit error rates (BERs), limited bandwidth, user contention, radio interference, and TCP traffic rate management. A QoS-aware wireless system is desired to address all these problems.

Detailed Description Text (20):
2. Service In data networking, a service can be defined as a type of connection from one end of a network to another. Formerly, this could have been further defined to be protocol specific, such as, e.g., IBM's systems network architecture (SNA), Novell's IPX, Digital's DECnet. However, it appears that TCP/IP (i.e. including user datagram protocol(UDP)) has evolved to become the overwhelming protocol of choice, and will continue to be in the foreseeable future. Therefore, service can be defined to be a particular type of TCP/IP connection or transmission. Such service types might include, e.g., FTP file transfers, e-mail traffic, hypertext transfer protocol (HTTP) traffic, H.323 video conferencing sessions. It is desirable that a QoS mechanism deal with these differing types of service, in addition to dealing with the different types of quality as discussed previously.

Detailed Description Text (27):
Virtual circuits were to be established for data transmission sessions, again regardless of the data application or whether data was being transmitted at any given moment. Although ATM provides QoS for broadband network traffic, the underlying assumptions of ATM design include the low BER characteristic of wireline networks, not the high BER of the wireless medium. Without a recognition of the characteristics of the traffic that is being carried by the ATM mechanism and the high inherent BER of wireless, true QoS can not be provided. ATM QoS mechanisms do not address the unique challenges associated with wireless communication.

Detailed Description Text (63):
The TCP/IP protocol stack has become the standard method of transmitting data over the Internet, and increasingly it is becoming a standard in virtual private networks (VPNs). The TCP/IP protocol stack includes not only internet protocol (IP), but also transmission control protocol (TCP), user datagram protocol (UDP), and internet control message protocol (ICMP). By assuming that the TCP/IP protocol stack is the standard network protocol for data communications, the creation of a set of optimal QoS mechanisms for the wireless broadband data environment is more manageable. QoS mechanisms can be created that can span the entire extent of the network, including both the wireline and the wireless portions of the network. These mechanisms can integrate in a smooth and transparent manner with TCP rate control mechanisms and provide end-to-end QoS mechanisms that are adaptive to both the wireline and wireless portions of the network. Of course, segments of the wireline network that are congested or are experiencing other transport problems cannot be solved by a wireless QoS mechanism. However, a wireless QoS mechanism can optimize data flows in a manner that can enhance the end user experience when there is no severe wireline network congestion or bottleneck present.

Detailed Description Text (65):
Data traffic can be handled based on classes of service, as discussed above. To differentiate traffic by class, data traffic (or a sequence of data packets associated with a particular application, function, or purpose) can be classified into one of several classes of service. Differentiation can be done on the basis of some identifiable information contained in packet headers. One method can include analyzing several items in, e.g., an IP packet header, which can serve to uniquely identify and associate the packet and other packets from that packet flow with a

particular application, function or purpose. As a minimum, a source IP address, a source TCP or UDP port, a destination IP address, and a destination IP or UDP port can serve to associate packets into a common flow, i.e. can be used to classify the packets into a class of service.

Detailed Description Text (85):
In the wireless environment, with an appropriately designed MAC layer, packet loss due to BER that might otherwise trigger congestion collapse and global synchronization can best be managed with local retransmission of lost packets according to the present invention and without RED and the unnecessary retransmission of packets by the TCP sender and the resulting reset of TCP transmission rate. The IP-centric wireless system separately manages the TCP transmission window of the TCP sender remotely by transmitting a packet receipt-acknowledgment before the TCP sender detects a lost packet and initiates retransmission along with an unnecessary reset of the transmission rate. This IP-centric wireless system TCP transmission window manager communicates with the MAC layer in order to be aware of the status of all packets transmitted over the wireless medium.

Detailed Description Text (95):
The present invention's proactive reservation-based intelligent multimedia-aware media access (PRIMMA) media access control (MAC) layer provides an application switching function of the IP-centric wireless QoS mechanism. Once the nature and QoS requirements of each IP stream are determined by other portions of the system, this information is communicated to the PRIMMA MAC layer so that the IP flows of each application can be switched to appropriate destinations in a proper priority order.

Detailed Description Text (97):
For IP streams that originate from a local user's CPE, application-level information about the nature of the application can be used by the system to assign appropriate QoS mechanism parameters to the IP stream. For IP streams that originate from a non-local host, information about the IP streams for use in configuring the appropriate QoS mechanism parameters can be extracted from packet headers. The information about the IP streams is communicated "vertically" in the protocol stack model from the application layer (i.e. OSI level 7) to the PRIMMA MAC layer (i.e. OSI level 2) for bandwidth reservation and application switching purposes. Although this violates the conventional practice of providing isolation and independence to each layer of the protocol stack, thereby somewhat limiting the degree of interchangeability for individual layers of the stack, the advantages far outweigh the negatives in an IP-centric wireless broadband access system.

Detailed Description Text (116):
Network 200 further includes a fixed wireless CLEC 209. Example fixed wireless CLECs are Teligent Inc., of Vienna, Va., WinStar Communications Inc., Advanced Radio Telecom Corp. And the BizTel unit of Teleport Communications Group Inc. Fixed wireless CLEC 209 includes a wireless transceiver/receiver radio frequency (RF) tower 210 in communication over an RF link to a subscriber transciever RF tower 212. Subscriber RF tower 212 is depicted coupled to a CPE box, PBX 112b. PBX 112b couples calling parties 124b and 126b, fax 116b, client computer 118b and associated modem 130b, and local area network 128b having client computer 120b and server computer 122b coupled via an associated modem 130b.

Detailed Description Text (122):
To establish a connection with an ISP, client 118b can use a host computer connected to a modem (modulator/demodulator) 130b. The modem can modulate data from the host computer into a form (traditionally an analog form) for transmission to the LEC facilities. Typically, the LEC facilities convert the incoming analog signal into a digital form. In one embodiment, the data is converted into the point-to-point protocol (PPP) format. (PPP is a well-known protocol that permits a

computer to establish a connection with the Internet using a standard modem. It supports high-quality, graphical user-interfaces.) As those skilled in the art will recognize, other formats are available, including, e.g., a transmission control program, internet protocol (TCP/IP) packet format, a user datagram protocol, internet protocol (UDP/IP) packet format, an asynchronous transfer mode (ATM) cell packet format, a serial line interface protocol (SLIP) protocol format, a point-to-point (PPP) protocol format, a point-to-point tunneling protocol (PPTP) format, a NETBIOS extended user interface (NETBEUI) protocol format, an Appletalk protocol format, a DECnet, BANYAN/VINES, an internet packet exchange (IPX) protocol format, and an internet control message protocol (ICMP) protocol format.

Detailed Description Text (128):
Alternatively, trunks can include optical carriers (OCs), such as OC-1, OC-3, etc. Table 3 provides typical optical carriers, along with their respective synchronous transport signals (STSs), ITU designations, and bandwidth capacities.

Detailed Description Text (136):
In the SS7 network, the SSPs are the portions of the backbone switches providing SS7 functions. The SSPs can be, for example, a combination of a voice switch and an SS7 switch, or a computer connected to a voice switch. The SSPs communicate with the switches using primitives, and create packets for transmission over the SS7 network.

Detailed Description Text (157):
Currently, internets, intranets, and similar public or private data networks that interconnect computers generally use packet switching technology. Packet switching provides for more efficient use of a communication channel than does circuit switching. Packet switched networks transport packets of information which can include various types of data such as, e.g., digitized voice, data, and video. With packet switching, many different calls can share a communication channel rather than the channel being dedicated to a single call. During a voice call, for instance, digitized voice information might be transferred between the callers only 60% of the time, with silence being transferred the other 40% of the time. With a circuit switched connection, the voice call could tie-up a communications channel that could have 50% of its bandwidth, unused because of the silence. For a data call, information might be transferred between two computers only 10% of the time. With the data call, 90% of the channel's bandwidth may go unused. In contrast, a packet-switched connection would permit the voice call, the data call and possibly other call information to all be sent over the same channel.

Detailed Description Text (158):
Packet switching breaks a media stream into pieces known as, for example, packets, cells or frames. Each packet can then be encoded with address information for delivery to the proper destination and can be sent through the network. The packets can be received at the destination and the media stream is reassembled into its original form for delivery to the recipient. This process is made possible using an important family of communications protocols, commonly called the Internet Protocol (IP).

Detailed Description Text (162):
Network routers can include tables describing various network domains. A domain can be thought of as a local area network (LAN) or wide area network (WAN). Information can be transferred between a plurality of LANs and/or WANs via network routers. Routers look at a packet and determine from the destination address in the header of the packet, the destination domain of the packet. If the router is not directly connected to the destination domain, then the router can route the packet to the router's default router, i.e. a router higher in a hierarchy of routers. Since each router has a default router to which it is attached, a packet can be transmitted through a series of routers to the destination domain and to the destination host bearing the packet's final destination address.

Detailed Description Text (164):
A local area network (LAN) can be thought of as a plurality of host computers interconnected via network interface cards (NICs) in the host computers. The NICs are connected via, for example, copper wires so as to permit communication between the host computers. Examples of LANs include an ethernet bus network, an ethernet switch network, a token ring network, a fiber digital data interconnect (FDDI) network, and an ATM network.

Detailed Description Text (165):
A wide area network (WAN) is a network connecting host computers over a wide area. In order for host computers on a particular LAN to communicate with a host computer on another LAN or on a WAN, network interfaces interconnecting the LANs and WANs must exist. An example of a network interface is a router discussed above.

Detailed Description Text (166):
A network designed to interconnect multiple LANs and/or WANs is known as an internet (with a lower case "i"). An internet can transfer data between any of a plurality of networks including both LANs and WANs. Communication occurs between host computers on one LAN and host computers on another LAN via, for example, an internet protocol (IP) protocol. The IP protocol is used to assign each host computer of a network, a unique IP address enabling packets to be transferred over the internet to other host computers on other LANs and/or WANs that are connected to the internet. An internet can comprise a router interconnecting two or more networks.

Detailed Description Text (173):
Some networks are packet-centric networks. Unlike a circuit-centric network, a packet-centric network does not use dedicated circuits through which to transfer packets. TCP/IP performs a packetization of user data to be sent between and among the various systems on the IP network. When a large file is sent down the protocol stack, the IP function is responsible for segmentation and packetization of the data. Then a header is placed on the packet for delivery to the data link. The routing and switching of this data is handled at the IP (i.e. network) layer. IP is in a sense a dumb protocol. When a packet is prepared for transmission across the medium, IP does not specifically route the call across a specific channel. Instead, it places a header on the packet and lets the network deal with it. Therefore, the outward bound packets can take various routes to get from a source to a destination. This means that the packets are in a datagram form and not sequentially numbered as they are in other protocols. IP makes its best attempt to deliver the packets to the destination network interface; but it makes no assurances that data will arrive, that data will be free of errors, and that nodes along the way will concern themselves with the accuracy of the data and sequencing, or come back and alert the originator that something is wrong in the delivery mechanism. It is possible that in IP routing of a packet, the packet can be sent along the network in a loop, so IP has a mechanism in its header information to allow a certain number of "hops" or what is called "time to live" on the network. Rather than permit an undeliverable pack to loop around the network, IP has a counter mechanism that decrements every time the packet passes through a network node. If the counter expires, the node will discard the packet. Working together with IP is TCP which provides controls to ensure that a reliable data stream is sent and delivered. At the sending end, TCP puts a byte count header on information that will be delivered to the IP protocol layer and encapsulates it as part of the packet. The receiving end, when it gets packets is responsible for resequencing the packets and ensuring its accuracy. If all of the IP flow is not received correctly, the byte count acknowledgment or nonacknowledgment message can be sent back to the sending end, prompting the sending end to resend the bytes necessary to fill in the remaining portions of the packet flow. TCP buffers additional packets until after resending the nonacknowledged packet.

Detailed Description Text (176):
It is important to note that CATV is a wireless communication method. The frequencies of many video signals are distributed along the cable at the same time. A television tuner selects a particular channel by tuning into a specific frequency or a "frequency band."

Detailed Description Text (187):
In an example embodiment, data network 142 can be an IP packet-switched network. A packet-switched network such as, e.g., an IP network, unlike a circuit-switched network, does not require dedicated circuits between originating and terminating locations within the packet switched network. The packet-switched network instead breaks a message into pieces known as packets of information. Such packets can then be encapsulated with a header which designates a destination address to which the packet must be routed. The packet-switched network then takes the packets and routes them to the destination designated by the destination address contained in the header of the packet.

Detailed Description Text (188):
Routers 140a, 140b, 140c, 140d, 140e, 140f and 140g can be connected to one another via physical media such as, for example, optical fiber link connections, and copper wire connections. Routers 140a-g transfer information between one another and intercommunicate according to routing protocols.

Detailed Description Text (198):
ATM permits standardization on one network architecture defining a multiplexing and a switching method. Synchronous optical network (SONET) provides the basis for physical transmission at very high-speed rates. ATM can also support multiple quality of service (QoS) classes for differing application requirements by providing separate virtual circuits for different types of traffic, depending on delay and loss performance. ATM can also support LAN-like access to available bandwidth.

Detailed Description Text (214):
In an embodiment, data network 142 can be an internet protocol (IP) network over an ATM network. It would be apparent to those skilled in the art, that an internet protocol (IP) network over various other data link layer network such as, e.g., Ethernet, could be used as data network 142. Rather than transporting data in fixed length ATM circuit-centric cells, data could be transported in variable length IP datagram packet-centric packets as segmented by TCP. The IP data network can lie above any of a number of physical networks such as, for example, a SONET optical network.

Detailed Description Text (220):
The H.323 Recommendation for video conferencing will now be briefly overviewed. The H.323 standard provides a foundation for, for example, audio, video, and data communications across IP-based networks, including the Internet. By complying with the H.323 Recommendation, multimedia products and applications from multiple vendors can interoperate, allowing users to communicate without concern for compatibility. H.323 promises to be the foundation of future LAN-based products multimedia applications.

Detailed Description Text (223):
H.323 is part of a series of communications standards that enable videoconferencing across a range of networks. Known as H.32X, this series includes H.320 and H.324, which address ISDN and PSTN communications, respectively.

Detailed Description Text (226):
All H.323 terminals also support H.245, which is used to negotiate channel usage and capabilities. Three other components are required: Q.931 for call signaling and call setup, a component called Registration/Admission/Status (RAS), which is a

protocol used to communicate with a gatekeeper; and support for RTP/RTCP for sequencing audio and video packets.

Detailed Description Text (230):
Gateways are not required if connections to other networks are not needed, since endpoints may directly communicate with other endpoints on the same LAN. Terminals communicate with gateways using the H.245 and Q.931 protocols.

Detailed Description Text (232):
Many gateway functions are left to the designer. For example, the actual number of H.323 terminals that can communicate through the gateway is not subject to standardization. Similarly, the number of SCN connections, the number of simultaneous independent conferences supported, the audio/video/data conversion functions, and inclusion of multipoint functions are left to the manufacturer. By incorporating H.323 gateway technology into the H.323 specification, the ITU has positioned H.323 as the means to hold standards-based conferencing endpoints together.

Detailed Description Text (234):
Gatekeepers perform two important call control functions. The first is address translation from LAN aliases for terminals and gateways to IP or IPX addresses, as defined in the RAS specification. The second function is bandwidth management, which is also designated within RAS. For instance, if a network manager has specified a threshold for the number of simultaneous conferences on the LAN, the gatekeeper can refuse to make any more connections once the threshold is reached. The effect is to limit the total conferencing bandwidth to some fraction of the total available; the remaining capacity is left for e-mail, file transfers, and other LAN protocols. A collection of all terminals, gateways, and multipoint control units which can be managed by a single gatekeeper are known as an H.323 Zone.

Detailed Description Text (237):
A gatekeeper is not required in an H.323 system. However, if a gatekeeper is present, terminals must make use of the services offered by gatekeepers. RAS defines these as address translation, admissions control, bandwidth control, and zone management.

Detailed Description Text (246):
FIG. 2D depicts network 296 including a point-to-multipoint (PtMP) wireless network 298 coupled via router 140d to data network 142. It is important to note that network 296 includes network 286 from FIG. 2C, plus PtMP wireless network 298. PtMP wireless network 298 enables customer premise equipment (CPE) at a subscriber location to gain access to the various voice, data and video resources coupled to data network 142 by means of wireless connectivity over a shared bandwidth. The wireless PtMP network 298 is a packet switched network which is TCP/IP packet-centric (i.e. no dedicated circuit is created in delivering a communication IP flow) and QoS aware.

Detailed Description Text (247):
Specifically, PtMP wireless network 298 includes a wireless access point (WAP) 290d coupled to router 140d by, e.g., a wireline connection. A wireless access point 290e can be similarly coupled to router 140e by a wireline connection. WAP 290d is in wireless communication, such as, e.g., radio frequency (RF) communication, with one or more wireless transciever subscriber antennae 292d and 292e. It would be apparent to those skilled in the art that various wireless communication methods could be used such as, e.g., microwave, cellular, spread spectrum, personal communications systems (PCS), and satellite.

Detailed Description Text (248):
In an alternative embodiment, RF communication is accomplished over cable

television (CATV) coaxial cable. As those skilled in the relevant art will understand, a coaxial cable functions as a waveguide over which RF waves propagate. Accordingly, it is possible for the communications link between RF transceiver subscriber antenna 292d and WAP 290d to be a coaxial cable. Therefore, a coaxial cable connection is analogous to a wireless connection, and is referred to as an alternative form of wireless connection in the present invention.

Detailed Description Text (249):
In another alternative embodiment, RF communication is accomplished over a satellite connection, such as, e.g., a low earth orbit (LEO) satellite connection or a high earth orbit satellite. Taking the example of an LEO satellite connection, WAP 290d and RF transceiver subscriber antenna 292d function as satellite gateways, with the additional functionalities described in the present invention.

Detailed Description Text (253):
In an embodiment of the invention, either of antennae 292d and 292e can communicate with both WAPs 290d and 290e for alternate or backup wireless communications paths.

Detailed Description Text (254):
Returning to FIG. 3A, it depicts an example perspective diagram 300 of a PtMP network of the present invention. Diagram 300 includes a wireless base station 302 shown in wireless communication with subscriber locations 306a, 306b, 306c, 306d, 306e, 306f, 306g, 306h, 306i and 306j. Specifically, wireless base station 302 communicates via wireless access point 290d to subscriber antennae 292a-j of subscriber locations 306a-j.

Detailed Description Text (256):
Returning to FIG. 3B, it depicts block diagram 310 further illustrating the wireless PtMP of the present invention. Diagram 310 includes wireless base station 302 coupled at interface 320 to data network 142. Also coupled to data network 142 are router 140d and telephony gateway 288b which is in turn coupled to a class 5 central office (CO) switch at EO 104b. IP telephony gateway 288b can terminate telephony traffic to PSTN facilities by, e.g., translating packets into time domain multiplexed (TDM) standard telephone signals. Wireless base station 302 is in communication with wireless CPE 294d at subscriber location 306d via antenna WAP 290d and 292d. It would be apparent to those skilled in the art that other configurations of CPE 294d are possible, such as, e.g., one or more host computers with no telephone devices, one or more telephones with no host computers, one or more host computers and one or more telephone devices, and one or more H.323 capable video-conferencing platforms which could include a host computer with monitor and camera.

Detailed Description Text (266):
Network layer 408 is the Internet protocol (IP) 429. As will be discussed further below and as already discussed above with reference to data network 142, IP is a standard protocol for addressing packets of information. Referring now to FIG. 7, IP header fields 702 can include, e.g., source and destination IP addresses, IP type of service (TOS), IP time to live (TTL), and protocol fields. IP is a datagram protocol that is highly resilient to network failures, but does not guarantee sequence delivery. Routers send error and control messages to other routers using the Internet control message protocol (ICMP). ICMP can also provide a function in which a user can send a "ping" (echo packet) to verify reachability and round trip delay of an IP-addresse host. Another OSI layer 3 protocol is address resolution protocol (ARP) which can directly interface to the data link layer. ARP maps a physical address, e.g., an Ethernet MAC address, to an IP address.

Detailed Description Text (268):
IP 429 of network layer 408 can be, e.g., an IP version 4 (IPv4) or an IP version 6 (IPv6). IPv6 (sometimes called next-generation internet protocol or IPng) is a

backward-compatible extension of the current version of the Internet protocol, IPv4. IPv6 is designed to solve problems brought on by the success of the Internet (such as running out of address space and router tables). IPv6 also adds needed features, including circuiting security, auto-configuration, and real-time services similar to QoS. Increased Internet usage and the allocation of many of the available IP addresses has created an urgent need for increased addressing capacity. IPv4 uses a 32-byte number to form an address, which can offer about 4 billion distinct network addresses. In comparison, IPv6 uses 128-bytes per address, which provides for a much larger number of available addresses.

Detailed Description Text (271):
Resource reservation protocols that operate on a per-connection basis can be used in a network to elevate the priority of a given user temporarily. RSVP runs end to end to communicate application requirements for special handling. RSVP identifies a session between a client and a server and asks the routers handling the session to give its communications a priority in accessing resources. When the session is completed, the resources reserved for the session are freed for the use of others.

Detailed Description Text (274):
Because RSVP provides a special level of service, many people equate QoS with the protocol. For example, Cisco currently uses RSVP in its IPv4-based internetwork router operating system to deliver IPv6-type QoS features. However, RSVP is only a small part of the QoS picture because it is effective only as far as it is supported within a given client/server connection. Although RSVP allows an application to request latency and bandwidth, RSVP does not provide for congestion control or network-wide priority with the traffic flow management needed to integrate QoS across an enterprise. Further, RSVP does not address the particular challenges related to delivering packets over a wireless medium.

Detailed Description Text (279):
RTP and other Internet real-time protocols, such as the Internet stream protocol version 2 (ST2), focus on the efficiency of data transport. RTP and other Internet real-time protocols like RTCP are designed for communications sessions that are persistent and that exchange large amounts of data. RTP does not handle resource reservation or QoS control. Instead, RTP relies on resource reservation protocols such as RSVP, communicating dynamically to allocate appropriate bandwidth.

Detailed Description Text (281):
Real-time Control Protocol (RTCP) is a companion protocol to RTP that analyzes network conditions. RTCP operates in a multi-cast fashion to provide feedback to RTP data sources as well as all session participants. RTCP can be adopted to circumvent datagram transport of voice-over-IP in private IP networks. With RTCP, software can adjust to changing network loads by notifying applications of spikes, or variations, in network transmissions. Using RTCP network feedback, telephony software can switch compression algorithms in response to degraded connections.

Detailed Description Text (285):
Real-time transport protocol (RTP) is currently an IETF draft, designed for end-to-end, real-time delivery of data such as video and voice. RTP works over the user datagram protocol (UDP), providing no guarantee of in-time delivery, quality of service (QoS), delivery, or order of delivery. RTP works in conjunction with a mixer and translator and supports encryption and security. The real-time control protocol (RTCP) is a part of the RTP definition that analyzes network conditions. RTCP provides mandatory monitoring of services and collects information on participants. RTP communicates with RSVP dynamically to allocate appropriate bandwidth.

Detailed Description Text (306):
1. Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP)

Detailed Description Text (309):
Transport layer four 410 can include transmission control protocol (TCP) or user datagram protocol (UDP) 427 part of the standard TCP/UDP/IP protocol family suite of networking protocols. As will be discussed further below and as already mentioned briely above with reference to data network 142, TCP is a standard protocol for segmenting traffic into packets, transmitting, reassembling and retransmitting packets of information between a source and destination IP address. Referring now to FIG. 7, TCP header fields 706 can include, e.g., source and destination port numbers, window size, urgent pointer, flags (SYN, ISN, PSH, RST, FIN), and maximum segment size (MSS). Both TCP and UDP provide a capability for the TCP/IP host to distinguish among multiple applications through port numbers. TCP can provide for a reliable, sequenced delivery of data to applications. TCP can also provide adaptive flow control, segmentation, and reassembly, and prioritization of data flows. UDP only provides unacknowledged datagram capability. The recently defined real time protocol (RTP), RFC 1889, can provide real time capabilities in support of multimedia applications, for example.

Detailed Description Text (323):
Uplink PRIMMA MAC segmentation and resequencing (SAR) and framer 636 (hereinafter SAR and framer 636) can segment and frame the data packets of IP flows into frames for transmission over the wireless medium from CPE 294 at CPE subscriber locations 306 to wireless base station 302 for further transmission over data network 142. IP flow 626 from CPE 294d at CPE subscriber location 306d can be transmitted to base station antenna 290d over a wireless medium such as, e.g., RF communication, cable modem and satellite communication, from subscriber antenna 292d coupled to CPE 294d at CPE subscriber location 306d.

Detailed Description Text (340):
As noted, multiple applications can be connected to one or more subscriber CPE stations at subscriber CPE locations 306a-306e. To prevent collisions between multiple applications contending for a fixed number of bandwidth allocations for uplink communication, in one embodiment of the present invention a reservation scheduling system is used. The bandwidth allocations for data packets are called frame slots, and are described below with respect to FIGS. 12A-12Q, 14, 16A and 16B.

Detailed Description Text (346):
In the reservation scheduling function of this embodiment, each subscriber CPE station requests the reservation of frame slots for its uplink transmissions using a reservation request block (RRB) of the TDMA airframe, described further below with reference to FIGS. 12A-12O, before it is permitted to communicate in the uplink path with interface 320. After the reservation request, uplink flow scheduler 634 transmits, as indicated by line 640, to the requesting subscriber CPE station 294 a description of one or more slots which the CPE station 294 can use to transmit its uplink data packets from source subscriber workstations 120, over the wireless medium, which are directed toward destination host workstations 136, over data network 142.

Detailed Description Text (395):
Referring to FIG. 12N, performance data 1248a comprises the number of comrepeats 1252a (the number of repeats of communication attempts), number of frameslips 1252b (the number of frames that have slipped), waitstate index 1252c (an index to the waiting state).

Detailed Description Text (404):
In the present invention, an advanced reservation algorithm assigns future slots to data packets based on the priority of the IP data flow with which the packet is associated. Exemplary priorities are described above with respect to FIGS. 8A and 8B. For calls that are sensitive to jitter, meaning calls that are time sensitive,

it is important to maintain an isochronous (i.e., in phase with respect to time) connection. With such signals, it is important that the data be dispersed in the same slot between frames, or in slots having a periodic variation between frames. For example, vertical reservation 1480 shows a jitter sensitive signal receiving the same slot for downlink communications in each frame. Specifically, the signal is assigned slot 1422 in frames 1402-1416. If the frame-to-frame interval is 0.5 ms, then a slot will be provided to the IP flow every 0.5 ms. As another example, diagonal reservation 1482 shows a jitter sensitive signal receiving a slot varying by a period of one between sequential frames. Specifically, the signal is assigned slot 1440 in frame 1402, slot 1438 in slot 1404, . . . slot 1426 in frame 1416, to create a "diagonal." If the frame-to-frame interval is 0.5 ms and the slot-to-slot interval is 0.01 ms, then a slot can be provided to the IP flow every 0.5 minus 0.01, equals 0.49 mms. Thus, to decrease the frame interval, a diagonal reservation of positive slope can be used. To obtain an increased frame interval, a diagonal of negative slope such as, e.g., negative slope diagonal uplink reservation 1486. The diagonal reservation 1482 can also be more pronounced (i.e., using a greater or lesser slope), depending on the period between sequential frames desired. Reservation patterns 1480, 1482, 1484 and 1486 are useful patterns for jitter sensitive communications. Also illustrated is a vertical reservation 1486, similar to vertical reservation 1480, useful for a jitter sensitive communication in the uplink direction.

Detailed Description Text (406):
For calls that are less latency sensitive, fewer slots per frame can be assigned for the communication. For example, a communication that is less latency sensitive can receive a guaranteed bandwidth of one slot every four frames. A call that is even less latency sensitive can receive, e.g., a single slot every ten frames.

Detailed Description Text (423):
If not, meaning that the IP flow is a new IP data flow, then control passes to module 1524, where the packet header fields are analyzed. Module 1524 analyzes the packet header source field and determines from source application packet header data table 1528 the type of source application making the data call or transmitting the IP packet. The application can be any of the applications described with respect to FIG. 2D or known to those skilled in the art. Examples include a file transfer protocol (FTP) download from another client workstation 138f, an IP voice telephony call (over telephony gateway 288b), a voice telephony call from a caller 124d (connected over a modem), an e-mail from a LAN 128a attached host workstation 136a, a fax machine call, and a conference call from multiple callers 124d and 126d (connected over a modem), to name a few. If the IP flow is not known to the system, then the IP flow is given an IP flow identifier number, and control passes to module 1526 where the IP flow identifier number is added to the existing IP flow identification table 1526.

Detailed Description Text (429):
After processing by module 1532, in module 1536 a destination CPE subscriber station ID lookup from subscriber CPE IP address table 1538, is performed for the IP flow. Each subscriber CPE station 294d can have one or more applications, running on one or more subscriber workstations 120d, homed to it. Accordingly, the IP flows can be directed to one or more applications on one or more subscriber workstations of one or more CPE stations 294d. A subscriber workstation can be any device coupled to a subscriber CPE station 294d. Module 1536 looks up the IP flow in table 1538, to determine the identity of the subscriber CPE station 294d that will receive the packets of the new IP flow from data network 142. Control then passes from module 1536 to module 1542 of the packet classification component 1506.

Detailed Description Text (466):
Each time a subscriber CPE station 294d attempts to communicate in the uplink direction with wireless base station 302, it requests a reservation by inserting an

RRB in the uplink subframe. Uplink frame scheduler 634 then schedules the reservation request in a future uplink subframe and notifies the CPE station 294d of the reservation. In a downlink signal, uplink flow scheduler 634 located preferably at wireless base station 302, transmits a reservation slot in a particular future frame for the requesting subscriber CPE station 294d to transmit its uplink data. Uplink flow scheduler 634 assigns the reservation based on the same parameters as the downlink flow scheduler 604 uses in the downlink. In other words, uplink flow scheduler 634 determines the reservation slots based on the queue class priority and based on a set of rules, schedules the reservations for uplink transmissions from subscriber CPE station 294d using, e.g., an advanced reservation algorithm. The rules are determined by inputs to the uplink flow scheduler 634 from a hierarchical class-based priority processor module 1674, a virtual private network (VPN) directory enabled (DEN) data table 1672, and a service level agreement (SLA) priority data table 1670. The advanced reservation algorithm is described with respect to FIG. 14.

Detailed Description Text (491):
In one embodiment, uplink flow scheduler 634 is physically located in wireless base station 302, although those skilled in the art will recognize that the same functionality can be located remotely from wireless base station 302. For example, in another embodiment, uplink flow scheduler 634 can be located at CPE station 294d and is in communication with other CPE stations 294 and the wireless base station 302.

Detailed Description Text (505):
TCP is a reliable transport protocol tuned to perform well in traditional networks where congestion is the primary cause of packet loss. However, networks with wireless links incur significant losses due to bit-errors. The wireless environment violates many assumptions made by TCP, causing degraded end-to-end performance. See for example, Balakrishnan, H., Seshan, S. and Katz, R. H., "Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks," University of California at Berkeley, Berkeley, Calif., accessible over the Internet at URL, http://www.cs.berkeley.edu/.about.ss/papers/winet/html/winet.html, dealing more directly with handoffs and bit errors in a narrowband wireless environment, the contents of which are incorporated by reference. Attempts to address this problem have modified TCP in order to overcome it. However, this is not a commercially feasible means of overcoming this challenge. It is impracticable to implement any solution that requires a change to the standard operation of TCP.

Detailed Description Text (506):
The present invention uses an enhanced MAC layer which interfaces with a TCP adjunct agent to intercept TCP layer requests to manipulate the TCP layers at either a source or destination end of a transmission, to modify TCP behavior at the source and destination of the TCP/IP transmission which includes an intermediary wireless link. Packets can be queued at the wireless base station awaiting receipt acknowledgment and the base station can perform local retransmissions across the wireless link to overcome packet loss caused by high bit-error rates. Communication over wireless links is characterized by limited bandwidth, high latencies, sporadic high bit-error rates and temporary disconnections which must be dealt with by network protocols and applications.

Detailed Description Text (509):
The present invention maintains packets in class queues awaiting acknowledgment of receipt from the subscriber CPE stations. Unacknowledged data slots can then be resent by having the wireless base station perform local retransmissions to the subscriber CPE station. By using duplicate acknowledgments to identify a packet loss and performing local retransmissions as soon as the loss is detected, the wireless base station can shield the sender from the inherently high bit error rate of the wireless link. In particular, transient situations of very low communication quality and temporary disconnectivity can be hidden from the sender.

Detailed Description Text (518):
TCP/UDP layers 510a and 510f act to provide such transport functions as, e.g.,segmentation, managing a transmission window, resequencing, and requesting retransmission of lost packet flows. Normally TCP layers 510a and 510f would send a window of packets and then await acknowledgment or requests for retransmission. A TCP sliding window algorithm is normally used to vary the transmission flow to provide optimized transport and to back off when congestion is detected by receipt of requests for retransmission. Unfortunately in the wireless environment, due to high bit error rates, not all packets may reach the destination address, not because of congestion, but rather because of high bit error rates, so as to prompt a retransmission request from the destination IP host to the source. Rather than slow transport, TCP adjunct agent 510e modifies operation of the TCP sliding window algorithm to optimize operation over wireless. PRIMMA MAC layer 504d interacts with TCP adjunct agent 510e permitting the agent to intercept, e.g., retransmission requests, from TCP layer 510a of subscriber workstation 120d intended for host 136a, and allowing the wireless base station to retransmit the desired packets or flows to subscriber workstation 120d rather than forwarding on the retransmission request to host 136a, since the packets could still be stored in the queue of PRIMMA 504d and would not be discarded until an acknowledgment of receipt is received from the subscriber CPE. Since retransmission can be performed according to the present invention at the PRIMMA MAC data link layer, i.e. layer 2, retransmission can occur from the base station to the CPE subscriber, rather than requiring a retransmission from all the way over at the transmitting source TCP which would cause TCP to backoff its sliding window algorithm. Thus, by having wireless base station 302 retransmit until receipt is acknowledged over the wireless link, the inherently high bit error rate can be overcome, while maintaining an optimal TCP window.

Detailed Description Text (521):
In the event that real congestion occurs, i.e. if the TCP adjunct agent recognizes packets really were lost, then the TCP adjunct agent can let the retransmission request go through to the transmitting TCP. This is advantageously accomplished because the MAC link layer of the present invention is in communication with the higher protocol layers, it is application aware, transport aware and network aware. In this case, because the MAC layer is transport layer aware, PRIMMA MAC layer 504d communicates with the TCP adjunct agent 510e at layer 4. Since the MAC requires acknowledgment of receipt of wireless transmissions sent to the CPE subscriber station 294d for every packet sent from the wireless base station 302, the MAC layer 504d knows whether an inter-TCP layer communication, e.g., a request for retransmission, is sent from a client computer TCP at the CPE station is created because the lost packet was lost in wireless transmission, or because of real congestion.

Detailed Description Text (576):
Subscriber CPE 294d flows packets coming in from NIC 1802b, back up its protocol stack through Ethernet layer 1804b, through optional PPP layer 1806b to IP layer 1808b and 1808c, back down through an Internet firewall and IPsec security gateway 1806c, down through PRIMMA MAC 1804c to wireless physical layer 1802c including antenna 292d, then over the wireless medium, such as, e.g., RF communication, cable RF, and satellite link, to antenna 290d of wireless base station 302 at wireless physical layer 1802d.

Detailed Description Paragraph Table (4):
TABLE 3 Electrical signal, International Optical or synchro- Telecommuni-cations Bandwidth in carrier (OC) nous transport Union (ITU) Megabits per signal signal (STS) terminology second (Mbps) OC-1 STS-1 51.84 OC-3 STS-3 STM-1 155.52 OC-9 STS-9 STM-3 466.56 OC-12 STS-12 STM-4 622.08 OC-18 STS-18 STM-6 933.12 OC-24 STS-24 STM-8 1244.16 OC-36 STS-36 STM-12 1866.24 OC-48 STS-48 STM-16 2488.32

Other Reference Publication (20):
Cheng et al., "Wireless Intelligent ATM Network and Protocol Design for Future Personal Communication Systems", IEEE 1997.

Other Reference Publication (21):
Zahedi, A. et al. "Voice and Data Integration on TCP/IP Wireless Networks" Personal, Indoor and Mobile Radio Communication Sep. 1-4, 1997, vol. 2, pp. 678-682.

CLAIMS:

1. A packet-centric wireless point to multi-point telecommunications system comprising: a wireless base station coupled to a first data network; one or more host workstations coupled to said first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with said wireless base station over a shared wireless bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of said subscriber CPE stations over a second network; resource allocation means for optimizing end-user quality of service (QoS) and allocating said shared wireless bandwidth among said subscriber CPE stations, wherein said resource allocation means is application aware, and wherein said application awareness comprises awareness of at least one layer above layer 4 of Open Systems Interconnect (OSI) model; and means for analyzing and scheduling an internet protocol (IP) flow over said shared wireless bandwidth, wherein said scheduling means comprises: prioritization means for prioritizing said IP flow in comparison to other IP flows based on priorities of a virtual private network (VPN) associated with said IP flow.

9. A scheduling method for use in a packet-centric wireless point to multi-point telecommunications system, said telecommunications system comprising: a wireless base station coupled to a first data network; one or more host workstations coupled to said first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with said wireless base station over a shared wireless bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of said subscriber CPE stations over a second network; resource allocation means for optimizing end-user quality of service (QoS) and allocating said shared wireless bandwidth among said subscriber CPE stations, wherein said resource allocation means is application aware, and wherein said application awareness comprises awareness of at least one layer above layer 4 of Open Systems Interconnect (OSI) model; means for analyzing and scheduling an internet protocol (IP) flow over said shared wireless bandwidth, wherein said scheduling method comprises the steps of: prioritizing said IP flow in comparison to other IP flows based on priorities of a virtual private network (VPN) associated with said IP flow.

19. A packet-centric wireless point to multi-point telecommunications system comprising: a wireless base station coupled to a first data network; one or more host workstations coupled to said first data network; one or more subscriber customer premise equipment (CPE) stations in wireless communication with said wireless base station over a shared wireless bandwidth using a packet-centric protocol; and one or more subscriber workstations coupled to each of said subscriber CPE stations over a second network; a resource allocator to optimize end-user quality of service (QoS) and allocate said shared wireless bandwidth among said subscriber CPE stations, wherein said resource allocator is application aware, and wherein said application awareness comprises awareness of at least one layer above layer 4 of Open Systems Interconnect (OSI) model; and a scheduler to schedule an internet protocol (IP) flow over said shared wireless bandwidth, wherein said scheduler comprises: a prioritizer to prioritize said IP flow in comparison to other IP flows based on priorities of a virtual private network (VPN) associated with said IP flow.

h e b b g e e e f c e fhgc e ge